National Aeronautics and
Space Administration

OSP-PLAN-0009
BASELINE
EFFECTIVE DATE: September 10, 2003

George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama 35812

UP01

ORBITAL SPACE PLANE PROGRAM
RISK MANAGEMENT PLAN

MSFC - Form 454 (Rev. October 1992)

Orbital Space Plane Program Risk Management Plan
Approval Signatures

Prepared By :

Rosalie W. Allen — Date
Manager
Program Planning and Control Office

Approved By:

Shannon D. Bartell — Date
Orbital Space Plane Assistant Program Manager
Kennedy Space Center

David C. Leestma — Date
Orbital Space Plane Assistant Program Manager
Johnson Space Center

Dennis E. Smith — Date
Orbital Space Plane Program Manager
Marshall Space Flight Center

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Baseline		9/10/03	Baseline Release

TABLE OF CONTENTS

PARAGRAPH **PAGE**

List of Figures

List of Tables

1 Introduction

OSP Program activities are focused in two main areas:

- Design, Development, and Production of the Orbital Space Plane system
- Technology and Flight Demonstrations

The Design, Development, and Production element of the OSP Program began the formulation phase in FY03. Per NPG 7120.5B Guidelines, the Formulation Phase will be utilized to establish the Program schedule and budget plans. The current budget planning is based on formulation concept studies being conducted in FY03 and FY04, preliminary design activities conducted in FY04 and FY05, a System Definitions Review (SDR) in FY04, and a Preliminary Design Review in FY05. A decision whether to enter into implementation (proceed with the Full Scale Development) of the OSP is scheduled to be made at end of FY04 following the SDR, completion of Non-Advocate Review (NAR), and completion of an Independent Cost Review including a Cost Analysis Requirements Document (CARD). At that point, a decision to proceed will result in the OSP Program transitioning from Formulation to Implementation.

The objective of the Technology and Flight Demonstrations program element is to provide the necessary flight demonstrations and technology development activities to enable the OSP development. Demonstrations will validate thermal effects, autonomous capabilities, design/manufacturing techniques, and crew escape capabilities across a range of demonstrators designed to mature critical technologies through test and evaluation. Demonstrators currently planned include the X-37, the Demonstration of Autonomous Rendezvous Technology (DART), and the Pad Abort Demonstrator (PAD).

1.1 PURPOSE

This Risk Management Plan adheres to the requirements of NPG 7120.5, NASA Program and Project Management Processes and Requirements and MWI 7120.6, Program/Project Risk Management.

The purpose of this document is to provide personnel across the program with a clear, concise description of how the OSP Program will manage risk. This document is organized as follows:

- An overview of the continuous risk management process.
- The identification of OSP Program characteristics that determine the risk management methodology applied.
- The standard role of every organization in risk management.

- Details on how to effectively utilize the risk management functions and processes.

This document describes the methodologies and processes used to identify, analyze, plan, track, control, communicate and document the OSP Program's risks. The identification, characterization, mitigation plan, and mitigation responsibilities associated with specific risks are contained in the OSP risk database (discussed in Section 5.1) and specific risk mitigation or contingency plan documents.

1.2 SCOPE

This document is applicable to the entire NASA OSP Program and OSP interfaces with the International Space Station (ISS) Program, and Launch Service Program (LSP). ISS and LSP have there own risk management programs and are not covered within the scope of this Risk Management Plan, except to define interfaces. The X-37 and the Demonstration of Autonomous Rendezvous Technology (DART) projects have there own risk management programs and are not covered within the scope of this Risk Management Plan. This is the Program's Risk Management Plan from acquisition through Program completion. It assumes that the Integrated Risk Management Application (IRMA) is the risk management database application used to document and communicate risk.

1.3 ASSUMPTIONS, CONSTRAINTS, AND POLICIES

This plan addresses methods and tools used in the risk management process and the initiation of risk management procedures across the OSP Program. It is expected that changes and improvements will be necessary over the course of time to reach a Risk Management Capability Maturity Model (RM-CMM) Level III (see Appendix), i.e. a well-defined, repeatable risk management process. Objective evidence will be collected to demonstrate the risk management plan is implemented. The risk management process will use both qualitative risk assessment and Quantitative Risk Assessment (QRA) techniques as described in section 4.4.1. Corrections should be forwarded to the OSP Program Risk Manager.

1.4 APPLICABLE DOCUMENTS

The Orbital Space Plane Program Plan directs the activities of the overall program. The Risk Management Plan is subordinate and integral to the Program Management Plan.

- NPG 7120.5 NASA Program and Project Management Processes and Requirements
- NPG 8000.4 Risk Management Procedures and Guidelines
- NPD 2810.1 Security of Information Technology
- NPG 2810.1 Security of Information Technology

- NPD 2820.1 NASA Software Policy
- OSP-PLAN-005 OSP Program Plan
- OSP-DOC-040 OSP Configuration Management Plan
- OSP-DOC-030 OSP Data Management Plan

1.5 Reference Documents

- MWI 7120.6 Program/Project Risk Management
- SSP 30234 Failure Modes and Effects Analysis/Critical Items List (FMEA/CIL) for Space Station
- NPG 8715.3 NASA Safety Manual
- OSP-PLAN-0XX OSP Probabilistic Risk Assessment (PRA) Plan
- NPG 8705 Human Rating Requirements and Guidelines for Space Flight Systems
- OSP-DOC-001 OSP Level 1 Requirements Interpretation Document
- LSP-OSPDEV-0001 OSP to Expendable Launch Vehicle (ELV) Interface
- MSFC-ICD-3361 ISS to OSP Interface Control Document Part I
- K-ELV-12.2 Rev A Expendable Launch Vehicle (ELV) Launch Services Project Risk Management Plan
- SSP 50175 Rev A ISS Risk Management Plan
- EIA 731 Systems Engineering Capability Model (SECM)
- *Continuous Risk Management Guidebook*. Dorofee, Audrey j., Julie A. Walker, Christopher J. Alberts, Ronald P. Higuera, Richard P. Murphy, and Ray C. Williams. Software Engineering Institute, Carnegie Mellon University, 1996.
- *Risk Management Maturity Level Development*. Risk Management Research and Development Program Collaboration: INCOSE Risk Management Working Group; Project Management Institute Risk Management Specific Interest Group; UK Association for Project Management Risk Specific Interest Group, April, 2002.

1.6 ACRONYMS

AMO .....Acquisition Management Office

CARD…….Cost Analysis Requirements Document

CDR .....Critical Design Review

CIL .....Critical Items List

CIO.....Chief Information Officer

COTR.....Contracting Officer Technical Representative

CPMC .....Center Program Management Council

CRM.....Continuous Risk Management

DART.....Demonstration of Autonomous Rendezvous Technology

ECP .....Engineering Change Proposal

EIA.....Electronic Industries Alliance

ELV.....Expendable Launch Vehicle

EMS .....Chief Engineer and Mission Success Office

EVM.....Earned Value Management

FMEA .....Failure Modes and Effects Analysis

FSD .....Full Scale Development

FTA.....Fault Tree Analysis

GPMC .....Governing Program Management Council

HA.....Hazard Analysis

IGCE……...Independent Government Cost Estimate

IOC.....Initial Operating Capability

IPT.....Integrated Product Team

IRMA .....Integrated Risk Management Application

ISS.....International Space Station

JSC .....Johnson Space Center

KSC.....Kennedy Space Center

LSP.....Launch Services Program

MCO .....Mars Climate Orbiter

MIB.....Mishap Investigation Board

MSFC.....Marshall Space Flight Center

NAR……Non-Advocate Review

NASA……. National Aeronautics and Space Administration

NPD.....NASA Program Directive

NPG.....NASA Program Guideline

NWI.....NASA Work Instruction

OSP .....Orbital Space Plane

PAD.....Platform Abort Demonstrator

PCB .....Program Control Board

PDR.....Preliminary Design Review

PIO .....Program Integration Office

PP&C .....Program Planning and Control

PRA.....Probabilistic Risk Assessment

QRA .....Quantitative Risk Assessment

R-BAM……Risk-Based Acquisition Management

RCG .....Risk Classification Grid

RDO .....Requirements Development Office

RE .....Risk Exposure

RFP……. Request For Proposals

RLV.....Reusable Launch Vehicle

RM .....Risk Manager

RM-CMM .....Risk Management Capability Maturity Model

RMT.....Risk Management Team

SAPHIRE.....Systems Analysis Programs for Hands-on Integrated Reliability Evaluations

S&MA.....Safety and Mission Assurance

SEB…….Source Evaluation Board

SECM…….Systems Engineering Capability Model

SE&RD .....Systems Engineering and Requirements Definition

SEI.....Systems Engineering and Integration

SDR…….System Definitions Review

SOW……Statement of Work

SOO…….Statement of Objectives

SRD…….Systems Definition Review

SRR…….Systems Requirements Review

TBQ.....Taxonomy-Based Questionnaire

WBRM.....Web Based Risk Management

WBS.....Work Breakdown Structure

1.7 DEFINITIONS

Affinity Grouping Method: the affinity grouping method groups risks that are naturally related and identifies the one concept that ties each grouping together. Groups of risks may share a common mitigation plan. See chapter A-2 of the *Continuous Risk Management Guidebook* for a detailed discussion of Affinity Grouping.

Analysis of Risk: an evaluation of all identified risks to estimate the likelihood of occurrence, consequence of occurrence, timeframe when mitigation actions are needed, classification into sets of related risks, and priority ranking.

Avoid: a strategy to avert the potential of occurrence and/or consequence by selecting a different approach or by not participating in the program.

Baseline: initial documentation of a process or product which is placed under configuration control. Subsequent changes to baseline are called “revisions”.

Classification of Risks: 1) the process of grouping risks into high, moderate, and low categories based on the likelihood and consequence adjective ratings. High, moderate, and low risks are represented by the colors red, yellow, and green, respectively. 2) The process of grouping risks based on shared characteristics or relationships among risks. Classification helps to identify duplicate risks and supports simplifying the list of risks. Affinity grouping is a form of risk classification.

Concern: a potential risk that an individual has entered into the risk management database. Once a concern is validated it becomes a risk. A concern that has not been validated as a risk will be closed.

Initiative: an organizational block within any tier of the OSP Program structure.

Initiative Managers: the managers of the organizational blocks depicted in Figure 2.1.

Issue: a risk that has occurred, becoming a problem. Issues are managed in the corrective action system, not in the risk management system.

Problem: synonymous with issue. Problems/Issues put the Program in a reactive mode rather than the early identification of potential risks (proactive mode) advocated by the OSP risk management process.

Program Tiers:	Tier I	Program Management Office
	Tier II	Program Integration and other Functional Offices
	Tier III	Projects, Elements, and System Design Teams

Research: the investigation of an identified risk until there is enough information to know if the risk ownership is still assigned properly, and what to do about the risk (e.g., accept the risk, watch the risk, or mitigate the risk).

Reporting and Documenting Risks: an overt action to communicate and document the risk at all steps of the CRM process.

Risk: a measure of the potential inability to achieve overall program success within defined cost, schedule, and technical constraints and has two components: (1) the probability (or likelihood) of failing to achieve a particular outcome, and (2) the consequences (or impact) of failing to achieve that outcome.

Risk Identification: a continuous effort to capture, acknowledge, and document risks as they are found.

Risk Management: the act or practice of dealing with risk. It includes planning for risk, assessing (identifying and analyzing) risk areas, developing risk-handling options, monitoring risks to determine how risks have changed, and documenting the overall risk management program.

Risk Acceptance: the determination that the consequences of an identified risk, should they occur are acceptable without further mitigation. No further resources are expended in managing this risk.

Risk Control: an activity that utilizes the status and tracking information to make a decision about a risk or risk mitigation effort. A risk may be accepted, watched, researched, avoided, transferred, mitigated, or closed. A mitigation action may be re-planned, or a contingency plan may be invoked. Decisions on the appropriate resources needed are also determined during this Risk Control activity.

Risk Escalation: the process of raising risk attention by reporting the risk to a higher level in the organization. This is done either to raise the awareness and visibility of a risk, calling attention to adverse changes in consequence, likelihood of occurrence or timeframe, or to request resources are not available to handle the risk at the lower level. The risk would be escalated to one or more levels above the level at which it is owned and mitigated.

Risk Exposure: defined mathematically as the product of the likelihood and the consequence of occurrence. Risk exposure is used to classify risks, determine which risks are of significant magnitude to warrant a mitigation strategy, and to prioritize risks for reporting and management purposes.

Risk Management Team: consists of the initiative risk managers, OSP Program Risk Manager, and risk contractor support personnel. The RMT supports the OSP Program Office. This risk management team reviews top organizational risks that have been requested to be escalated to

the Program Office, by their risk owners. RMT examines risks to determine interrelationships among all risks.

Risk Mitigation: the elimination or reduction of an identified risk by reducing the consequences, by reducing the likelihood, or by shifting the timeframe.

Risk Owner: identifies, implements, and tracks the risk mitigation approach and actions. The risk owner, by definition, has the necessary resources (budget and workforce) required to mitigate the risk.

Risk Planning: establishes the proper course of action for dealing with a particular risk. The resulting actions are to research, watch, accept, transfer, avoid, or to mitigate the risk.

Risk Tracking: an activity to capture, compile, and report risk attributes and metrics which determine whether or not risks are being mitigated effectively and whether risk mitigation plans are being implemented correctly.

Success Criteria: the minimum set of measures that establish the accomplishment of predefined goals and objectives for a given activity or undertaking. Within the practice of risk management it usually refers to the establishment of goals and objectives for risks mitigation activities.

Task: a significant activity that has defined/approved goals, objectives, requirements, budget and schedule baseline, a beginning and an end. A task may be an in-house activity or a contracted effort.

Taxonomy Based Questionnaire: a list of interview questions organized according to the natural organization or breakdown of the program or initiative.

Threat: risks that could impact overall Program success, i.e., schedule milestones, technical objectives, and cost/budget limitations.

Top Organizational Risks: any risk at the Tier II level.

Top Program Risks: any risk at the Tier I level. Referred to as “primary risks” in NPG 8000.4.

Transfer: the act of allocating authority, responsibility, and accountability for a risk to another person or organization.

Validate Risk: the process of examining an identified concern to verify that it has been written in such a way as to allow further analysis and that mitigation actions are within the scope of the program or initiative in question.

Watch: the monitoring of an identified risk and its attributes for early warning of critical changes in consequences, likelihood, timeframe, or other aspects.

Risk Management Database Application: is a software application for storage, retrieval and processing of risk data. The tool can be used for creating reports for all OSP Program personnel, Tier III through Tier I, to retrieve data for day-to-day risk management. This is described in Section 5.1.

2 OSP Program Characteristics

This section provides an overview of the OSP Program. Information included here is relevant to tailoring a risk management process to fit the needs of the Program. Should any aspect of the organization change, then the plan should be assessed for relevancy.

2.1 OSP PROGRAM ORGANIZATION

The OSP Program Office consists of the OSP Program Manager at MSFC and Associate Managers at JSC and KSC. Five organizations report to the OSP Program Office: Requirements Development Office (RDO), Program Planning and Control (PP&C), Program Integration Office (PIO), Acquisition Management Office (AMO), and Chief Engineer and Mission Success Office (EMS). Reporting to the PIO Office are four Elements (Spacecraft Integration, Launch Site Integration, Operations Integration, and Concept Assessment and Optimization), three system design teams (managing Boeing, Lockheed Martin and Northrop Grumman/Orbital Sciences contractor teams), one technology demonstrator project (Pad Abort Demonstrator (PAD)), and the Systems Engineering and Integration Office (SEI). The organization is shown in Figure 1.

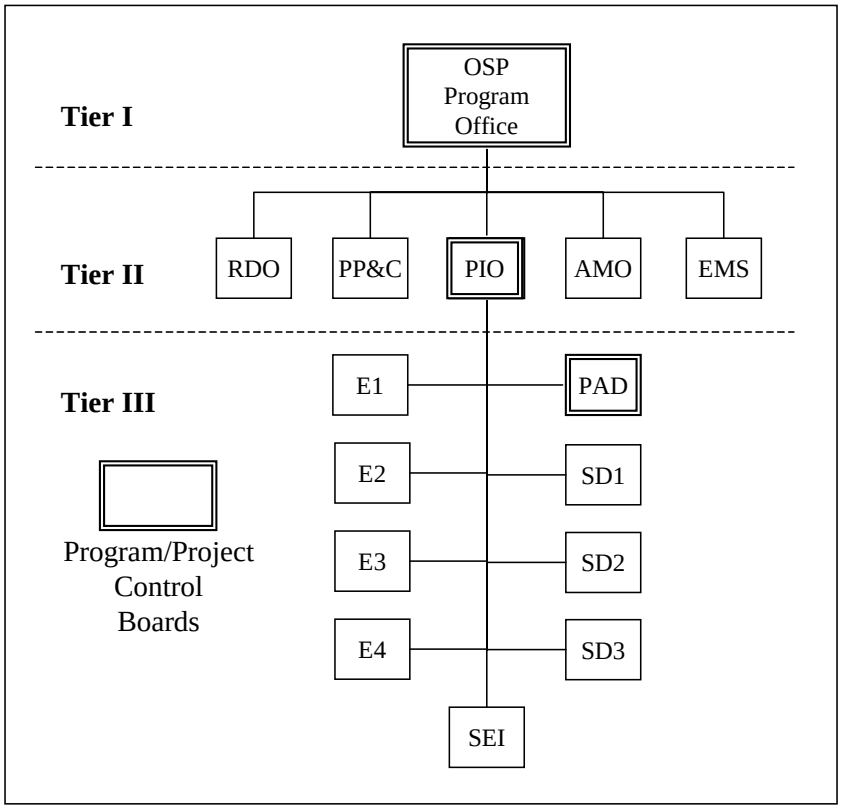

FIGURE 1. The OSP Organization.

The OSP Program Manager chairs an OSP Program Control Board to review and disposition changes to the OSP Program. Similarly, PIO Manager chairs a PIO Project Control Board to review and disposition changes to the Tier III initiatives.

2.2 OSP PROGRAM MANAGEMENT APPROACH

The OSP Program Management Approach is documented in the OSP Program Plan.

2.3 OSP ACQUISITION STRATEGY

The primary responsibility of the Acquisition Management Office (AMO) is the planning of the acquisition strategy for the full-scale development and operations of the OSP system. The AMO risk management is based on the Risk-Based Acquisition Management (R-BAM) process. An AMO Integrated Product Team (IPT) employs the R-BAM process to identify and address contract performance risks, acquisition process-related risks, and program level risks. AMO risks are associated with the program direction that the full-scale development contract must be awarded no later than August 1, 2004 in order to have an operational OSP (CRV mode) in 2008.

The OSP acquisition phase addresses requirements and acquisition strategy development. Major activities during this phase are:

- The development of Level 1 and Level 2 system requirements
- Validation of requirements through the Systems Requirements Review (SRR) and the Systems Definition Review (SDR), respectively
- Development of the contract Statement of Work (SOW) or Statement of Objectives (SOO)
- Development of the Independent Government Cost Estimate (IGCE)
- Writing of the full-scale development and operations Request For Proposals (RFP)
- Conducting the Source Evaluation Board (SEB)
- Obtaining approval to award the contract(s)

The AMO risk management team is responsible for assessing and mitigating the risks that may affect the required August 1, 2004 contract award. The AMO team is also responsible for assuring that the RFP for the development and operations phases includes requirements for risk management processes addressing all aspects of the OSP system flight hardware, ground operations, flight operations, and logistics systems.

2.4 OSP SUCCESS CRITERIA

The Risk Management Plan needs to meet the Success Criteria of the OSP Program Plan (OSP-PLAN-005).

2.5 OSP IDENTIFIED THREATS

Risk Management planning workshops were conducted with the Tier I OSP Program Office and all of the Tier II and III Initiative Managers and their staff. Threats were identified that could impact overall Program success. The risk management process was tailored to ensure that the identified threats could be accommodated within the risk management system.

3 PROCESS OVERVIEW

3.1 RISK MANAGEMENT ROLES, RESPONSIBILITIES, AND COMMUNICATION PATHS

Table I summarizes the responsibilities of program and initiative personnel performing CRM.

Roles	**Risk Management Responsibilities**
Individuals and Contractors	• Take OSP continuous risk management training • Identify potential risks
Risk Owner	• Estimate likelihood, consequence, and time frame • Classify risks • Collect and report general risk measures/metrics • Recommend approach and actions • Implement risk mitigation approach and actions • Track risks and mitigation plans (acquire, compile, and report) if assigned • Assist in risk prioritization • Performs the initial risk analysis once they are assigned ownership • Update risk information at least monthly and as status changes • If watch is recommended, the risk owner develops and defines the watch plan, and triggers. • If research is recommended, the risk owner develops the strategy, actions, responsibilities, and schedules, for conducting the research, evaluating, and reporting the results.
Initiative Risk Manager	• Initiative Manager's designated representative for risk management functions • Integrate risk information from all individuals within initiative's organization • Assign risk owner • Collect and report general risk measures/metrics • Coordinate communication within the initiative • Determines validity of an identified "concern" • Determines what action is most appropriate for treatment of the identified risk: further research, watch, transfer, avoid, accept, or mitigate • Transfers ownership within a Tier or requests escalation to the next higher Tier with Initiative Manager's approval

TABLE I. Program & Initiative Personnel Responsibilities.

Tier II and Tier III Initiative Managers	• Overall responsibility for risk management activities within their organization • Validate identified initiative level risks • Integrate risk information from all individuals within their organization • Ensure accuracy of likelihood/consequence/timeframe estimates and risk exposure classification • Review recommendations on mitigation approach and action • Obtain risk status from staff and report status to upper management • Prioritize initiative or task level risks • Assign or change responsibility for risks and mitigation plans to risk owner • Authorize transferal or escalation of risk • Evaluate and approve control decision recommendations • Evaluate and approve mitigation plans. • Collect and report general risk measures/metrics • Coordinate communication with the initiative office and OSP program office • Make and implement control decisions (analyze, decide, execute) • Authorize expenditures of initiative resources to mitigate risk
Program Risk Manager	• Responsible for overall risk management coordination • Chairs weekly meetings of the risk management team • Resides with the PP&C initiative • Ensures that new risk management products and tools are reviewed by the RMT • Ensures proper application of the risk management process and tools across the Program. • Ensures that the RMT integrates risk information from all initiatives.
OSP Program Office	• Overall responsibility for risk management activities within OSP Program • Responsible for initiating the transfer of risk to other Programs, if applicable • Validate identified program level risks • Authorize expenditures of management reserve for risk mitigation activities • Reprioritize risks from a Program perspective • Coordinate communication with stakeholders. • Review general risk measures/metrics during each quarter to evaluate the effectiveness of the risk management process

TABLE I. Program & Initiative Personnel Responsibilities (continued).

Table II provides the criteria for communicating and documenting risk information.

Communication Path	Risk to be Communicated/Documented
From Individuals, Teams, Contractors, and Task Managers to Tier III Initiative Managers	• Any risk that needs to be identified • Any risk that needs to be transferred to another team • Any risk that needs to be transferred to upper management • Risk mitigation process status
From Tier III Initiative Managers to Program Integration Office	• Any risk that needs to be transferred to another organization • Any risk that needs to be transferred to upper management • Highest priority risks of the initiative • Mitigation activity status • Risk Management process status
From Tier II Initiative Managers to Program Management Office	• Any risk that needs to be transferred to another Program • Any risk that needs to be transferred to upper management • Highest priority risks in the program • Any risk that is negatively impacting NASA's reputation • Overall Risk Mitigation Status • Risk Management Process Status

TABLE II. Communication Criteria.

3.1.1 OSP CONTRACTOR RISK MANAGEMENT RESPONSIBILITIES

Each of the managing organizations may have contractor organizations in support of their activities. The contractors are responsible for implementing a risk management process to manage their internal risks. This process must be compatible with the risk management procedures described in this OSP Risk Management Plan.

Risks identified by the contractor, which impact the Program, must be reported to the Contracting Officer's Technical Representative (COTR) or the Initiative Risk Manager. The COTR or Initiative Risk Manager will then identify the risks to the OSP Program. The risks are then processed as if entered by any other individual within the OSP Program.

The contractors COTR is responsible for providing the assessment of risk management performance, but requires input from the initiatives within the OSP Program that interface with the contractor. The contract may specify intervals at which assessment is provided to the contractor. If it is unspecified, then feedback should be provided at least quarterly. Initiative Risk Managers should assess the contractor risk management performance against their risk management requirements in the contract. In the absence of specific requirements, then the Initiative Risk Manager can use the Checklist for Assessment of Risk Management in Appendix C of NPG 8000.4, Risk Management Procedures and Guidelines. The method of delivery from the Initiative Risk Manager to the COTR is determined by the COTR.

3.1.2 EXTERNAL INTERFACES

TBD – Risk communication from OSP to LSP

TBD – Risk communication from OSP to ISS

3.2 RISK MANAGEMENT PROCESS

This section provides an overview of the Continuous Risk Management process as implemented by the Orbital Space Plane Program.

There are six primary activities within the CRM process, shown in Figure 2:

- Risk Identification is a continuous effort to capture, acknowledge, and document risks as they are found.

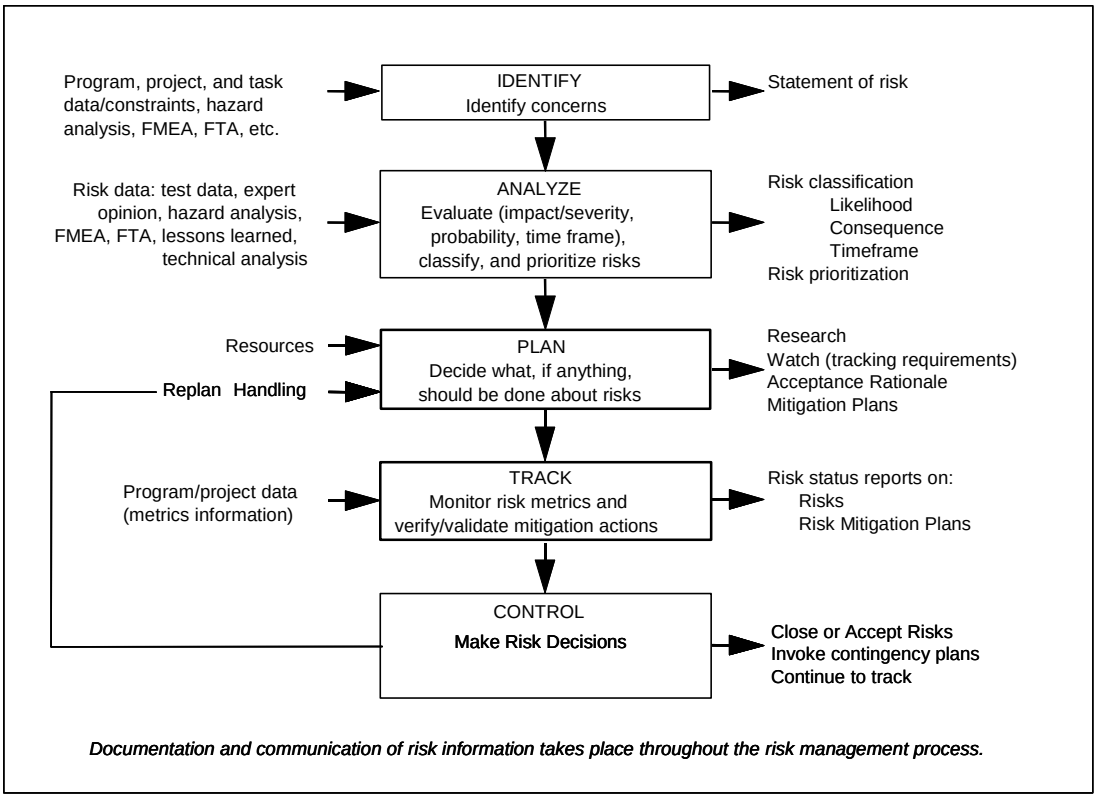

FIGURE 2. Continuous Risk Management Process Flow.

- Risk Analysis is an evaluation of all identified risks to estimate the likelihood of occurrence, consequence of occurrence, timeframe when mitigation actions are needed, classification into sets of related risks, and priority ranking.

- Risk Planning establishes the proper course of action for dealing with a particular risk. The resulting actions are to research, accept, watch, transfer, avoid, or to mitigate the risk

- Risk Tracking is an activity to capture, compile, and report risk attributes and metrics that determine whether or not risks are being mitigated effectively and whether risk mitigation plans are being implemented correctly.

- Risk Control is an activity that utilizes the status and tracking information to make a decision about a risk or risk mitigation effort. A mitigation action may be re-planned, or a contingency plan may be invoked. Decisions on the appropriate resources needed are also determined during this Risk Control activity.

- Risk Communication and Documentation is an overt action to communicate and document the risk at all steps of the CRM process.

Implementation procedures for the process are identified in Section 4.

3.3 OSP RISK MANAGEMENT INTEGRATION

The OSP Program Planning and Control Office (PP&C) is responsible for the coordination of all the OSP risk management products, processes, and tools. This office also coordinates any special risk activities requested by OSP Program management. Risk management integration is implemented between Tiers in the OSP Program organization by teams of risk coordinators from each initiative within the subordinate tier. That is, a risk management team consisting of Initiative Risk Managers from the Tier II organizations supports the Tier I OSP Program Office. A team of Initiative Risk Mangers from the Tier III organizations supports the Tier II Program Integration Office.

Initiative Risk Managers meet, at least bi-weekly, to discuss risk data. The purpose of this is twofold. First, based upon the gained awareness of Program risk, the team determines the appropriate level of management required to handle Program risks, ensuring vertical integration of risk data. Second, it allows Initiative Risk Mangers to communicate this information to their respective initiatives, thus facilitating horizontal integration of risk data.

The OSP Risk Manager resides within PP&C and is specifically responsible for risk management coordination. The OSP Risk Manager chairs weekly meetings of the RMT. The OSP Risk Manager ensures that schedules, new products, and tools are reviewed, and risk management process issues are decided by RMT and the managing organizations. Similar meetings are conducted by the Program Integration Office (PIO) Risk Manager to integrate risks owned by organizations supporting PIO. The PIO Risk Manager resides within the PIO initiative and chairs these meetings. The results of these weekly meetings are reported to the Initiative Manager on a monthly basis.

Figure 3 depicts the flow of information within an organization's Tier and between organizational Tiers. There are two reasons to escalate a risk to a higher Tier in the organization: if a risk owner within an initiative does not have the resources to manage a risk, or if the risk impacts Program reserves, Program milestones, or Level I requirements and requires visibility. For a risk owner in a Tier III organization, the request for escalation would be reviewed by the PIO risk management team. (Risks owned by Tier II owners are by default top organizational risks.) For a risk owner of a top organizational risk, the request to escalate to the Program Tier is reviewed by the Program Risk Management Team. If the Risk Management Team is unable to resolve any risk management issue, the issue is brought to the OSP Program Control Board.

The escalation of risks through the PIO risk management team and the OSP Risk Management Team effectively distributes the responsibility to manage risk. Risk Owners and Initiative Managers are allowed to exercise their good judgment with confidence that upper management trust them to do well. Only certain risks are escalated to higher levels and interdisciplinary teams determine when it is right to do so. This prevents Program Management from being deluged with risks that are already being handled. The tiered process is an effective and efficient way to integrate risk management within OSP.

As shown in Figure 3, Risk owners and their risk management teams communicate risk information and status to their initiative managers. The managers, with assistance from the risk management teams, prioritize the risks and apply resources to mitigate risk in the most effective and efficient manner. It is the responsibility of the risk owner to mitigate the risk in the manner deemed most appropriate.

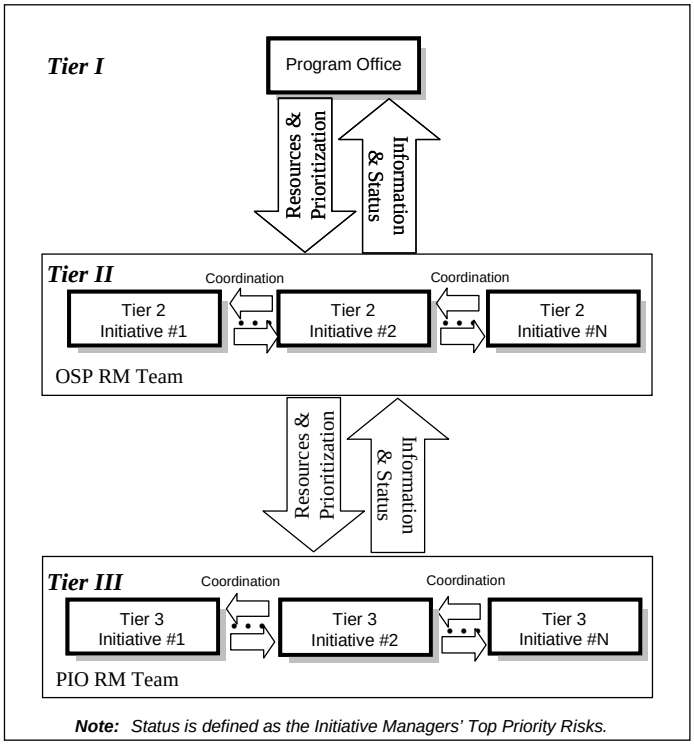

Figure 3. Risk Management Integration.

4 PROCESS DETAILS

The following sections provide detailed process steps for the CRM process that will be utilized for each Tier of the Orbital Space Plane Program. These steps apply to risk management performed at all levels.

4.1 RISK BASELINES

The initial list of Top Program Risks is established during the formulation phase of the Program. In determining the appropriate acquisition strategy, risks are solicited from the various initiatives, rolled-up through the Tiers to the Program Tier, and reported to acquisition officials, as part of Risk-based Acquisition Management, and NASA management. The risk baseline (Top Program Risks) will be discussed with prospective contractors to allow proposals to be evaluated based upon effective management of the risks, along with other factors.

Throughout the Program lifecycle, the list of Top Program Risks will be revised prior to major Program milestones. Incremental updates to the risk baseline are presented to the OSP Program Control Board at least quarterly.

4.2 IDENTIFYING RISKS

When a risk is entered into the system, it is initially considered a “concern”. The Initiative Risk Manager of the originator’s initiative is responsible for determining the validity of the risk. If the concern is valid, then it labeled a “risk” by the Initiative Risk Manager. Attempts are often made to use the risk management system to manage past problems or current issues. If an event has happened, or is certain to happen, then it should not be entered in as risk.

A valid risk is one that identifies a specific threat to the Program’s success criteria (see Section 2.4). All Tiers and individuals within the Program are responsible for identifying new risks. Risks shall be identified and entered as risk statements into the OSP Risk Management Database. A variety of methods may be used to identify risk, such as; Taxonomy Based Questionnaires (TBQ), work breakdown structure (WBS) risk assessment, team brainstorming, individual efforts, hazards analysis (HA), Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), and Lessons Learned. It is the responsibility of the individual initiative Managers to provide structured events designed to discover new risks and to ensure the timely entry of newly identified risks into the risk database. The database will warehouse, track, and report all risks. Every effort will be made to see that this system is compatible with existing contractor systems.

Risk statements consist of a description of the risk condition and the consequences of the risk. Risk statements shall be written clearly and concisely, citing only one risk condition, and one or more consequences of that condition. They typically take the following form: If ***A*** happens because of ***B***, then ***C*** will result. In the standard case, ***A is symptomatic***, ***B is causal***, and ***C is***

the result. A specific example is: Our ***software schedule could slip*** due to ***ill-defined requirements***, causing us to ***miss our Operational Readiness Review milestone***.

Once an Initiative Risk Manager deems a concern to be a valid risk, they assign the risk to a Risk Owner. A Risk Owner should be an individual from within OSP that has the resources (time and budget) and skills required to effectively analyze the risk, plan an appropriate handling strategy, and execute the handling strategy. The Initiative Risk Manager supports the Risk Owner in management of the risk and reporting risk management status.

The process steps contained in Table III shall be used to document and validate newly identified risks.

Step	Action
1	Concern is identified
2	Statement of risk is written for new risk in the proper format. The risk originator shall provide an initial estimate of the likelihood, consequence, and the timeframe of occurrence.
3	All information is input to the Risk Management database or equivalent contractor system.
4	A unique risk identifier is established automatically by the risk management database.
5	Risk statements entered into the database as concerns are reviewed weekly by the Initiative Risk Manager.
6	Valid concerns become a risk and are marked as “risks” by the Initiative Risk Manager. Invalid concerns are closed by the Initiative Risk Manager.
7	The Initiative Risk Manager assigns an initial ownership of the risk to a risk owner.

TABLE III. Documenting and Validating Risks Steps.

4.3 Analyzing Risks

All risks shall be analyzed to determine the likelihood and consequence of occurrence and the timeframe of when mitigation actions are needed. The risk consequence can be judged based upon cost, schedule, technical, and safety parameters. The risk owner is responsible for performing the initial risk analysis. The risks are also grouped by classification and can be consolidated as required. Risk Exposure (RE) is determined by mapping the likelihood of occurrence and the consequence of occurrence on a 5x5 matrix. This is described further in Section 4.3.1.

The Initiative Risk Manager, along with Initiative Manager, shall be responsible for further analyses and prioritization of risks identified within the initiative. Whether at the initiative Tier, PIO Tier, or Program Tier, risk management teams shall examine risks to determine interrelationships among the risks. Risks that relate directly with one another may be put into a risk set using the Affinity Grouping method and can be analyzed as a group.

The following process steps in Table IV shall be used to analyze risks.

Step	Action
1	Risk attributes (likelihood, consequence, and timeframe) shall be qualified by the assigned owner of the risk.
2	The assigned owner of the risk shall enter updates to the risk attributes into the risk management database.
3	Risks shall be prioritized by the Initiatives Risk Manager and Initiative Manager.
4	The initiative manager confirms ownership of the risk or assigns ownership to the appropriate individual. Appropriate manager affirms affinity grouping.

TABLE IV. Risk Analysis Steps.

4.3.1 CONSEQUENCE AND LIKELIHOOD

The output of the risk analysis process is the determination of likelihood and consequence of occurrence, and the timeframe in which action must be taken to mitigate the risk. Risks shall be analyzed using the Likelihood, Consequence/Impact, and Timeframe classifications as defined below. Consequence/Impact classifications are based on Orbital Space Plane Program requirements, initiative performance requirements, mission success criteria, resources, and cost and schedule constraints. Risk likelihood intends to provide an estimate based on available quantitative data and qualitative experience. Likelihood and Consequence coefficients are assigned values based on the descriptions listed below. Risk likelihood and consequence are subjectively scored using the magnitude column identified in Table V and Table VI below. Timeframe classifications are discussed in Section 4.3.2.

The risk scales are subjective ordinal scales, reflecting only relative standing between scale levels and not actual numerical differences. Any mathematical operations performed on results from ordinal scales, or a combination of ordinal and cardinal scales, can provide information that will at best be misleading, if not completely meaningless, resulting in erroneous risk ratings. Hence, mathematical operations should generally not be performed on scores derived from ordinal scales. Specifically, we do not multiply the likelihood and the consequence and attempt to derive meaning from the product.

The adjective ratings for risk likelihood are converted to numerical values for plotting on the 5x5 risk classification grid. The numerical equivalents to the adjective rating are the integer values from one (1) to five (5) with one being equivalent to “very low” and five being equivalent to “very high”. This is shown in Table V.

LIKELIHOOD	*What is the likelihood the situation or circumstance will happen ?*		
	Level	*Probability*	*. . . Or the current process . . .*
	5	Very High	cannot prevent this event, no alternative approaches or processes are available.
	4	High	cannot prevent this event, but a different approach or process might
	3	Moderate	may prevent this event, but additional actions will be required.
	2	Low	is usually sufficient to prevent this type of event.
	1	Very Low	is sufficient to prevent this event.

TABLE V. Likelihood of Occurrence Adjective Rating.

Each of the factors (i.e., safety, technical, cost, and schedule) must be considered when making a determination of risk consequence. The adjective ratings for risk consequence are also converted to numerical values for plotting on the 5 X 5 risk classification grid. The numerical equivalents to the adjective rating are the integer values from one (1) to five (5) with one being equivalent to "very low" and five being equivalent to "very high". The greatest numerical value for technical, cost, or schedule risk is taken to be the represent the overall qualification of the risk consequence. This is shown in Table VI.

CONSEQUENCE	*What is the Consequence (Cost, Schedule, Technical, or Safety) of this OSP* risk?					
	Level	1	2	3	4	5
	Cost	Minimal or no impact	Budget Increase < 5%	Budget Increase >5%	Budget Increase >10%	Budget Increase >15%
	Schedule	Minimal or no impact	Additional activities required. Able to Meet date.	Key Program milestone slip <= 1 month	Key Program milestone slip > 1 month, or Program critical path impacted	Cannot achieve Major Program milestone
	Technical	Minimal or no impact	Moderate Reduction, Same Approach Retained	Moderate Reduction, But Alternatives Available	Major Reduction, But Alternatives Available	Unacceptable, No Alternatives Exist
	Safety	•No Safety and Health Plan Violation •No adverse hazard or reliability change •Full regulatory compliance	•Documented CIL •Change in hazard controls but no increase in PRA •Minor violation of Federal or State regulation •<10% decrease in reliability	•CIL without acceptance rationale •Change in hazard controls with increase in PRA •Violation of Federal or State regulation •10-20% decrease in reliability	•Major but temporary injury •Potential damage to assets •Multiple violations of Federal or State regulation •>20% decrease in reliability	•Potential for permanent injury or death •Loss of critical assets •Willful or major violations of Federal or State regulation

TABLE VI. Consequence of Occurrence Adjective Rating.

A determination of Risk Exposure (RE) allows the consequence of occurrence and likelihood of occurrence to be expressed using one descriptor so that risk items may be classified, prioritized, and tracked. The risk exposure results in a "high", "moderate", or "low" risk classification, depending on where the risk falls on the Risk Classification Grid. As shown in Figure 4 the risk

exposure is considered high if the risk classification is in the red area, a moderate risk is shown in the yellow area, and a low risk classification is represented by green.

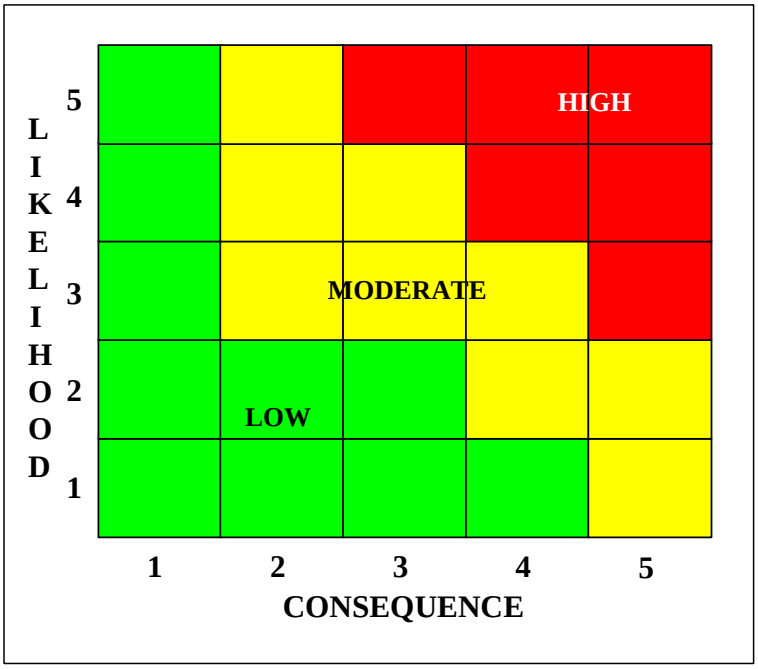

FIGURE 4. Risk Classification Grid.

4.3.2 TIMEFRAME CLASSIFICATION

Timeframe is used in conjunction with the Risk Exposure to determine priorities, establish when risks need to have actions taken. Timeframe is categorized as Near, Mid or Far term. This classification will be input into the risk database (discussed in Section 5.1) and the database will track any actions associated with the risks. The database will monitor by date when the risk was identified and when the timeframe classification of a risk changes. Risk classification changes will be automatically flagged by the database until an action is initiated for that risk.

Timeframe: When mitigation needs to commence.

- Near - Action or mitigation needs to take place within the next 3 months
- Mid - Action or mitigation needs to take place between 4 months and 8 months
- Far - Action or mitigation needs to take place beyond 8 months

4.4 RISK PLANNING

The Initiative Risk Manager is responsible for determining how to handle a risk and the risk owner is responsible for carrying out the handling strategy. Along with Initiative Manager and risk owner, the Initiative Risk Manager determines whether the risk owner has the resources available to handle the risk. If resources are not available, then the Initiative Risk Manager can request that the risk be escalated to the next Tier in the organization or request that adequate funding be provided to mitigate the risk. If the risk is escalated due to insufficient resources, then the risk ownership is transferred to someone in the higher Tier.

The Program Risk Manager, representing the Program Manager, is responsible for coordinating the prioritization of risks at the Program Tier and across all initiatives to determine the highest priority risks for the OSP Program as a whole. Final determination of OSP Program priorities is the responsibility of the Program Manager. In the analysis process step, only enough analysis was performed to accurately quantify the likelihood, consequence, and time frame of the risk and to confirm correct ownership. The objectives of the planning function are to make sure the consequences and sources of the risk are known, to develop effective plans, plan efficiently (only as much as needed or will have value), and to produce the correct set of actions that minimize risk and impacts while maximizing opportunity and value. Descriptions of risk handling options follow.

Risk mitigation plans must be included in the integrated schedules for the initiative and be allocated resources. This step integrates risk management into cost and schedule management processes within the Program. This is done for several reasons. First, synchronizing the mitigation plan with the initiative schedule assesses the timeliness of the mitigation. Second, incorporating it into the other management process allows for the mitigation tasks to be managed as part of the job and not a separate activity. Third, the budget assessment determines whether the cost to mitigate the risk is worth the impact of the initial risk, i.e. a cost-benefit assessment of the mitigation.

There is no electronic data interface between the risk management database application and the OSP budget and schedule systems. Duplicate data inputs into multiple systems may be required. The risk owner should remain mindful of this fact to prevent inconsistencies.

The following process steps in Table VII shall be used to plan for the control of risks.

Step	Action
1	The Initiative Risk Manager determines what action is most appropriate for treatment of the identified risk: further research, watch, transfer, avoid, accept, or mitigate.
2a	If research is recommended, the risk owner develops the strategy, actions, responsibilities, schedules, etc., for conducting the research, evaluating, and reporting the results.
2b	If watch is recommended, the risk owner develops the indicators, thresholds, and tracking requirements.
2c	If accept is recommended, the reasons for accepting the risk must be documented along with the current conditions and assumptions that support the decision by the risk owner.
2d	If a mitigation plan is appropriate, either an action item list or a task plan will be developed by the risk owner. Mitigation plans shall include, but not be limited to: definitive sets of activities, schedule, decision points, and contingency plans.
2e	If a risk is to be transferred, then the Initiative Risk Manager transfers ownership within a Tier or requests transfer to the next higher Tier.
3	All initiative Tier risk plans are reviewed and approved by the Initiative Manager and Initiative Risk Manager. Program Tier risk plans are reviewed and approved by the Program Manager and Program Risk Manager.
4	Resources for new tasks shall be identified and presented to the appropriate management team. Initiative reserve may be used if appropriate or new resources may be allocated to the initiative.

TABLE VII. Risk Planning Steps.

4.4.1 RESEARCH

Research is required to accurately estimate the likelihood or consequence of risk and to determine the most effective way to reduce either attribute. Risk arises from uncertainty and inexperience. It may be possible to effectively mitigate risk simply by enlarging the knowledge pool, leading to reassessment that reduces the likelihood of failure or provides insight into how to lessen the consequences.

The OSP Program intends to implement a capability to perform Quantitative Risk Assessment (QRA). QRA techniques attempt to accurately measure the impact of risk and help select the preferred handling approach. The quantitative techniques can be used in a point analysis or in trade studies. In a point analysis, QRA techniques assess the impact of risk on a given process or product to determine the “expected value” of the process or product. In trade studies, QRA techniques are applied to a suite of process or product options to determine the optimal outcome.

Two QRA techniques will definitely be used by the OSP Program to qualitatively assess risk. They are cost-schedule-technical risk analysis and probabilistic risk assessment (PRA). Other QRA techniques, such as decision trees, discrete event simulation, and multi-attribute utility functions, will be applied if OSP Program decision-making requires their application.

Cost-schedule-technical risk analysis is a QRA technique that quantifies the impact of risk on project costs. It is based on the underlying assumption that any technical objective can be met given sufficient resources. A scheduling tool that allows probabilistic distribution functions to be entered for task durations and resource costs is used to model the project and its risk. (Goldpan and @Risk for Project are commercially available tools for this type of modeling.) The model output is a probabilistic distribution function of the expected project cost and schedule. Information can be derived from the output to determine which risks have the greatest impact, which tasks have the greatest risk, the probability that a task will be on the critical path, etc.

PRA is a QRA technique that quantifies the impact of risk on the safety of the OSP. Tools that combine probabilistic risk and reliability are used to perform PRA. Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) is the tool that is used by the OSP Program. PRA tools use fault trees and event trees to model the probability of sub-system failure and the impact the failure will have on significant end-states, such as loss of crew or loss of vehicle. Information from the model can be derived to show which subsystems have the greatest impact on the end-states, which risks have the greatest impact, which mission scenarios are most likely to end in catastrophic end-states, etc.

Once the OSP Program begins Full Scale Development, both of these QRA techniques will be used to measure the programmatic and safety status of the Program. At least prior to major Program milestones, the models can be updated to demonstrate improvement in the risk environment and improved understanding within the Program of the risk drivers. For continuous decision support, the QRA techniques will be contribute to decisions on design options, risk handling options, and many other trade studies.

A plan that describes the OSP Program PRA approach is currently in development. A report detailing other QRA techniques and their application within the OSP Program is due in December 2003.

4.4.2 ACCEPT

One may accept the likelihood and the consequences associated with the risk's occurrence and decide to not mitigate the risk. Accepting risk is usually limited to low-level risks. It is usually not a "good" practice to accept moderate or high level risks. An exception is unfunded risk mitigation activities. These activities cannot be performed without budget. Therefore, unfunded risk mitigation activities mean that the risk is accepted (by definition) until the funding is authorized.

There may be Top Program Risks that the Program cannot effectively mitigate. Characterization of a Top Program Risk as "acceptable" shall be supported by the rationale, with the concurrence of the Governing Program Management Council (GPMC), that all reasonable mitigation options (within cost, schedule, and technical constraints) have been instituted.

An aggregate of low level risks that are accepted (or watched) can become a problem for the Program if they begin to materialize. A small lien against Program reserves should be set aside to handle these risks in case this happens.

4.4.3 WATCH

Often times the likelihood or consequence of a risk is small relative to the cost to mitigate the risk. Risks with a far-term timeframe may also be watched. However, risk exposure may grow if adverse trends continue. This type of risk is put on a watch lists to be monitored for growth in risk exposure. To "watch" a risk, one must determine some metric that can indicate a trend in risk exposure. Earned value management (EVM) metrics, such as the cost performance index and schedule performance index, are good indicators of increasing risk exposure. Thresholds are set to trigger mitigation plans when exceeded. Measures are then taken at regular intervals to "watch" the risk and see if the value exceeds the threshold.

4.4.4 TRANSFER

Transferal is a strategy to shift the risk to another area such as another requirement, initiative, external NASA Program, supplier, or stakeholder. Examples include reallocation of requirements, securing supplier product warranties, and negotiation of fixed-price contracts with suppliers. A risk can also be transferred to another initiative, in any tier, within OSP that is better equipped to handle the risk. The intent is to lower the risk exposure as a result of the risk transfer. Risks are transferred by identifying the appropriate owner, agreeing to the change in risk ownership, and finally changing the risk owner within the risk management application.

4.4.5 AVOID

Avoidance is a strategy to avert the potential of occurrence and/or consequence by selecting a different approach or by not participating in the program. Avoidance is different from mitigation. For example, mitigation attempts to reduce the likelihood or impact of a risk to a requirement whereas avoidance eliminates the requirement therefore eliminating the risk. The technique may be pursued when multiple designs or programmatic options are available. It is more likely used as the basis for a "go-no go" decision at the start of a program. Some examples are selection of state-of-the-practice rather than state-of-the-art technologies and pre-qualification of suppliers. The avoidance of risk is from the perspective of the overall program, which includes the stakeholders, contractors, and initiatives. Thus, an avoidance strategy is one that involves all of the major parties to the program and permits a program-wide avoidance of the risk.

4.4.6 MITIGATE

Risk mitigation does not attempt to eliminate the source of the risk but seeks to reduce or mitigate the risks. It monitors and manages the risk in a manner that reduces the likelihood and/or consequence of its occurrence or minimizes the risk's effect on the program. This option may add to the cost of a program; however, the selected approach should provide an acceptable risk level among the candidate approaches of risk reduction, cost effectiveness, and schedule impact. Should the mitigation required additional resources; a change request must be submitted per the Data Management Plan.

4.5 TRACKING RISKS

Risk tracking is performed to measure actual versus planned progress associated with implemented risk mitigation plans. The tracking process systematically tracks and evaluates the effectiveness of risk mitigation actions against established cost, schedule, safety, and technical performance metrics. Tracking results may also provide a basis for developing additional risk handling options and/or approaches, or updating existing risk handling strategies, and/or re-analyzing known risks. In some cases tracking results may also be used to identify new risks and revise some aspects of risk planning.

The key to the risk tracking process is to establish cost, schedule, safety, and technical performance management indicator metrics that the Initiative Manager and other key personnel use to evaluate the status of the program. These metrics are linked to the work processes or products, making it easy to determine the impact of an action. Risk indicator metrics should be established by each risk owner to provide early warning of potential problems to allow management actions. Risk tracking is not a problem-solving technique, but rather, a proactive technique to obtain objective information on the progress to date in reducing risks to acceptable levels. The following process steps in Table VIII shall be used to track risks.

Step	Action
1	The risk owner defines a mitigation plan for the risk
2	Risk mitigation schedule is included in initiatives' integrated schedule
3	Resources to conduct mitigation activities are accounted
4	Earned value metrics calculated on mitigation task
5	Integrated schedule, cost profile, and risk management database kept up-to-date with mitigation progress
6	Manager defines additional risk reports beneficial to judging overall risk environment and risk management progress. Reports are generated from database ad hoc or through pre-defined routines by Initiative Risk Manager.

Step	Action
7	Waterfall charts, earned value metrics, and other reports provided to management monthly to demonstrate progress, if necessary

TABLE VIII. Risk Tracking Steps.

4.6 CONTROLLING RISKS

Once the risk metrics and the mitigation action events have been chosen, risk management melds into program/project management and relies on program management processes to control the risk mitigation plans, correct for variations from the plans, respond to triggering events, and improve the risk management process. In fact, risk management must be integrated with day-to-day program management in order to be effective.

Monthly the Initiative Risk Manager reports tracking metrics to the Initiative Manager and jointly they determine if control measures, such as re-planning or contingency planning, are required. This is also the time when they may solicit the Program Office or the PIO for the allocation of additional resources to mitigate risks.

The following process steps in Table IX shall be used to control risks.

Step	Action
1	Risk Owner uses earned value reports to judge mitigation implementation progress and waterfall chart to judge mitigation product success
2	Mitigation contingency plans defined if failure seems inevitable
3	Reserves allocated to offset small deviations in mitigation plan

TABLE IX. Risk Control Steps.

5 Documentation and Risk Information

5.1 RISK MANAGEMENT DATABASE APPLICATION

The Program Office shall develop, maintain and update a risk management database application that will be utilized by the Program Office and all initiatives to identify, plan and track risks. This application will be web based and will provide consistency across the Program in performing CRM. All OSP initiative employees should have access to the risk management database application. They shall contact their Initiative Risk Manager for specific instructions to gain access.

The tool can be used for creating reports for all OSP Program personnel Tier III through Tier I to retrieve data for day-to-day risk management. This tool produces a set of standard reports for periodic reporting and has the ability to create ad hoc reports in response to special requests. The application also serves as a repository for all the risk information, serving as a lessons learned resource for current and future OSP Program Risk Management activities.

Figure 5 attempts to depict the life of a Tier III risk in the database application.

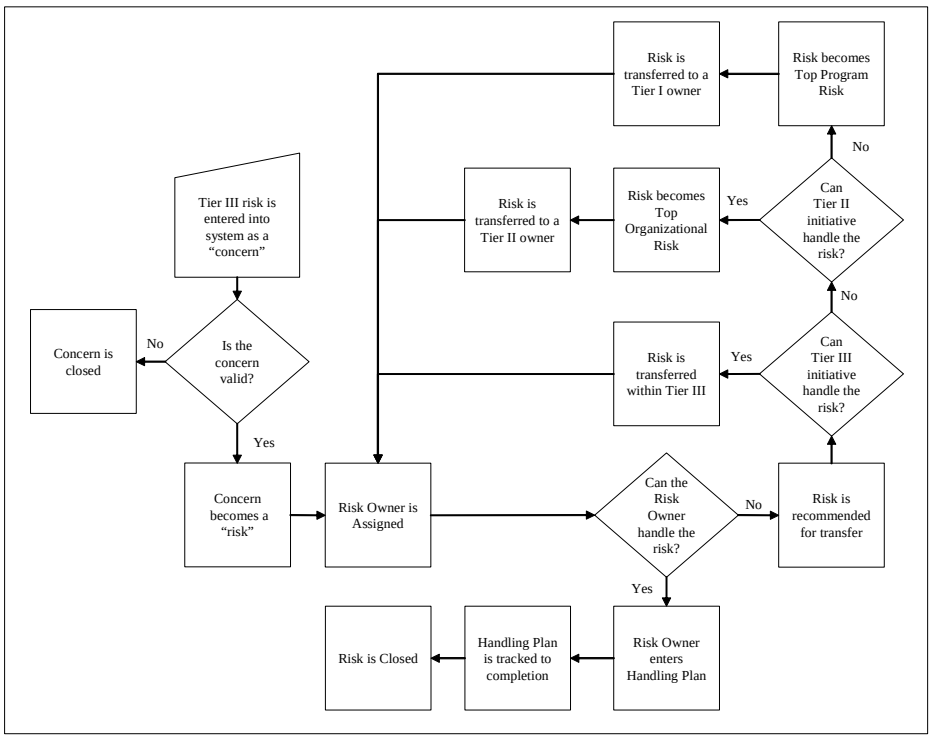

FIGURE 5. Life of a Tier III Risk in the Risk Management Database.

5.2 REPORTING AND DOCUMENTING RISKS

Weekly Program and/or initiative meetings will include status of risks. Monthly reporting of the risk status is required to convey information to the next highest tier. Risk information should also be reported if significant events occur between regular reporting intervals. The OSP Program Manager will make quarterly reports to senior management. Risk information shall be documented in the risk management database application, and will be made accessible to functional areas with data security protocols. Only the individuals with assigned responsibility for the risks shall have the authority to update the risk information and report the risk information. The reports are generated in Microsoft Word or Microsoft PowerPoint format.

The Initiative Risk Manager and the Initiative Manager determine the appropriate risk reports required to effectively manage the initiative. The Initiative Risk Manager maintains an archive (electronic or paper file) of the monthly risk management reports as objective evidence that the risk management plan is implemented.

Reports are generated for a category of risks in the database or for specific risks in the database. Categorized reports can cover all risks in the database or be limited to those risks pertaining to a particular organization. Categorized reports can also be filtered based upon several risk attributes, including risk exposure, risk type, inactivity, etc. Figure 6 is a Program Risk Summary Report summarizing the OSP risk environment at a given point in time.

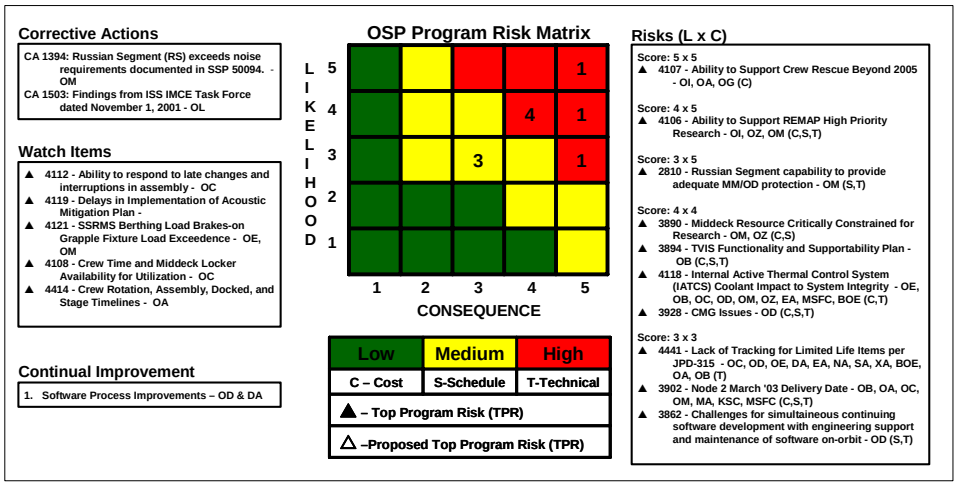

FIGURE 6. Program Risk Summary Report.

Figure 7 is a report of the risks in the database by the initiative, or organization affected by the risk. This report would allow the manager to identify areas within the organization that may require additional attention.

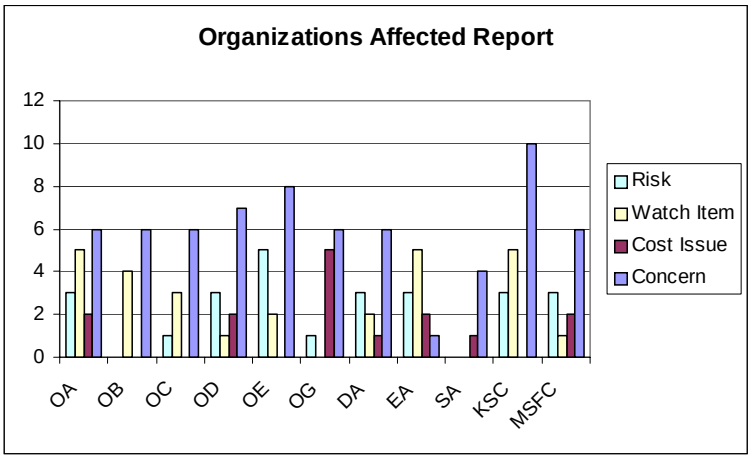

FIGURE 7. Organizations Affected Report.

Figure 8 is a report showing the improvement in risk classification of a particular risk on a waterfall chart. The waterfall chart allows the manager to see that a mitigation plan is in place for the risk, that progress is being tracked, and the status of that progress.

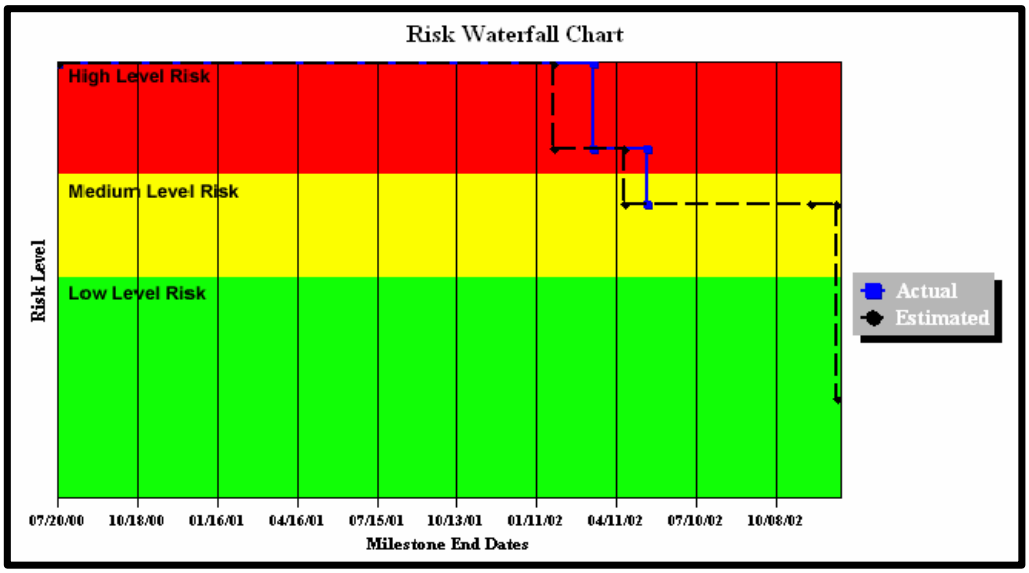

FIGURE 8. Risk Waterfall Chart.

6 OSP Program Risk Management Implementation

This section documents the process for putting the defined OSP Program Continuous Risk Management practice in place.

6.1.1 TRAINING

Training is an important element in the OSP Program risk management efforts to create a proactive, risk management culture. All OSP Risk Managers and employees shall receive training in risk management, as well as specific training in how to use the OSP risk management database application. Training will be provided by MSFC Safety and Mission Assurance (S&MA). Classroom courses will be conducted at the team member site.

6.2 OSP PROGRAM RESOURCES

This section identifies the resources required for the CRM activities.

Resources (cost, staff, equipment, software) for risk management activities shall be identified by the responsible risk owners. The resources for the management of risks can be broken down into two categories:

- Overhead costs and human resources associated with the setting up and establishing the risk management process for the initiative. The development, maintenance, and update of the Risk Management Plan and risk management database reside in this category.

- Risk control costs and human resources: resources associated with executing mitigation tasks and actions, resources allocated to planning, research and reporting. This includes the time required by the Risk Owner, Initiative Risk Manager, Program Risk Manager, and Risk Management Teams to perform their responsibilities.

6.3 SPONSORSHIP

The Orbital Space Plane Program Manager is supplying sponsorship for this effort.

6.3.1 SPONSORSHIP ROLES AND RESPONSIBILITIES

The sponsor shall provide continual, support for this effort at all Tiers of the organization. This shall include the following:

- Sponsor’s written endorsement and encouragement of this effort to all OSP Program personnel

- Monthly status review of risk management.

- The sponsor shall allocate budget to this effort

6.3.2 REPORTING REQUIREMENTS

The OSP Program Manager will make quarterly progress reports, as a minimum, to senior management on the implementation of the risk management system.

6.3.3 INFRASTRUCTURE ROLES

The following roles are required in order to support CRM in the Orbital Space Plane Program.

- **Risk Owner** – An individual that identifies, implements, and tracks the risk mitigation approach and actions. The risk owner will be provided the necessary resources (budget and workforce) required to mitigate the risk.

- **Program Risk Manager -** An individual from within the PP&C initiative, preferably at the managerial level, to provide motivation and leadership. Responsible for developing and implementing a CRM process that integrates all Program and initiative risk management activities, for managing the CRM process across the Program, and for ensuring the proper management of risks and open communication of risks as part of his/her routine activities.

- **Initiative Risk Manager -** An individual from within an initiative to provide motivation and leadership. Responsible for developing and implementing a CRM process that integrates all initiative risk management activities, for managing the CRM process across the initiative, and for ensuring the proper management of risks and open communication of risks as part of his/her routine activities.

- **Risk Contractor Support** – Skilled personnel hired as needed to support the CRM process.

6.4 CONTINUOUS RISK MANAGEMENT MILESTONES

The execution of the CRM process is broken down into two basic phases: the initial implementation phase, and the improvement phase.

6.4.1 IMPLEMENTATION PHASE

Initial continuous risk management implementation shall include the following:

- Database installed, tested, and all forms and templates to support the methods and tools incorporated

- Program Tier risk identification.

The detailed milestones for initial implementation are as follows:

- Prototype risk database is installed and tested.
- OSP Program specific risk management training provided.
- All initiatives have developed Risk Management Plans or have included an adequate discussion of the Project Risk Management process within their Project Plan.
- Individual access to database for risk identification is available and the database is being utilized.
- Weekly/monthly status meetings include risk as a discussion topic using reporting formats available from the database.
- Risk information is being maintained in the risk management database.

6.4.2 IMPROVEMENT PHASE

The following will be implemented during the improvement cycle.

- Monthly status meetings are reporting highest priority risk status to OSP Program Manager.
- Quarterly RM-CMM evaluations to determine need and scope for improvements to CRM process and CRM database. Develop plan for implementation of changes.
- Mitigation Status Report is provided.
- The CRM system is in place across the Orbital Space Plane Program with adequate reporting throughout the Program/Initiative.
- Measures/Metrics established to evaluate the successfulness of the CRM program.
- Integration of risk management with other management practices.
- Identification of risk management lessons learned, assessment of improvements, and development of improvement implementation plans.

6.5 EVALUATION MEASURES AND COMPLETION CRITERIA

6.5.1 IMPLEMENTATION PHASE

Initial implementation of a fully functional CRM process will be considered a success if the following outcomes have been achieved:

- OSP Program specific risk management training offered to all Program and initiative personnel, including non-MSFC personnel.

- All Program and initiative personnel have personal computer access to OSP risk management database.

- The Program monthly performance assessment teleconference agenda includes a status of the risk management process and status of risks for each initiative.

- All Program and initiative Tier risks identified are documented and tracked in the risk management database.

6.5.2 IMPROVEMENT PHASE SUCCESS CRITERIA

Improvement of the Orbital Space Plane CRM process will be considered successful if the following outcomes have been met:

- Top Program and initiative level risks are identified and tracked at the appropriate levels, and reported at the monthly performance assessment teleconference.

- Risk waterfall charts (shown in Figure 8) are developed and maintained for all Program and initiative Tier "red" and "yellow" risks.

- RM-CMM evaluation shows that the OSP has reached a RM-CMM Level III. Further improvements are identified and improvement plans are put into place.

7 Appendix: Risk Management Capability Maturity Model

Capability maturity models are designed to measure several aspects of an organization's capability to perform. The Risk Management Capability Maturity Model (RM-CMM) specifically measures an organization's capability to perform risk management. In general, RM-CMM is a model for judging the maturity of the risk management processes of an organization and for identifying the specific practices that are required to increase the maturity of these processes. Figure 9 shows the four level of risk management maturity.

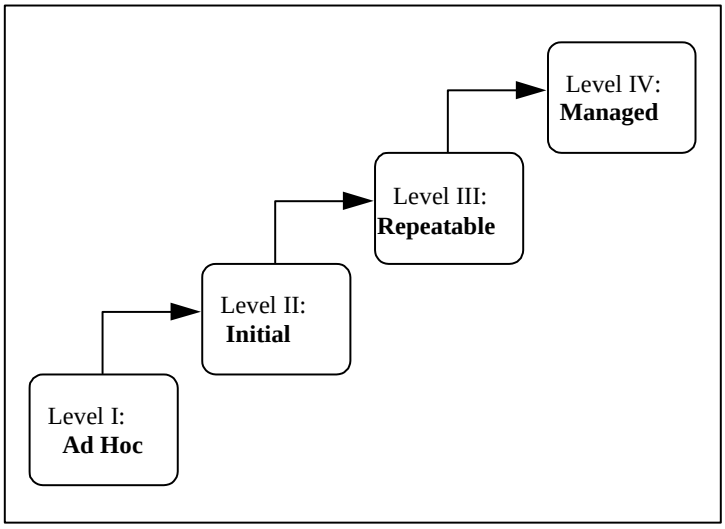

FIGURE 9. The Four Levels of Risk Management Maturity.

7.1 RM-CMM LEVELS

Brief descriptions of the RM-CMM levels are provided.

7.1.1 LEVEL I – AD HOC

At the Ad Hoc Level, the organization is unaware of the need for risk management and has no structured approach to dealing with uncertainty, resulting in a series of crises for each project or operation. Management and engineering processes, if they exist, are repetitive and reactive, with little or no attempt to learn from past projects or to prepare for future uncertainties. No attempt is made to identify risks to the project or to develop mitigation or contingency plans. The normal method for dealing with risk is to react after a problem occurs with no proactive thought.

7.1.2 LEVEL II – INITIAL

At the Initial Level, organizations are experimenting with the application of risk management, usually through a small number of nominated individuals within specific projects. At this level,

the organization has no formal or structured Risk Management process in place. Although the organization is aware, at some level, of the potential benefits of managing their project risks, there is no effectively implemented organization-wide process implemented. Some projects, those containing the nominated individuals, learn from past mistakes, however, there is no method implemented for providing these Lessons Learned to all of the organization's projects.

7.1.3 LEVEL III - REPEATABLE

At the Repeatable Level, the organization has implemented risk management into their routine business processes and implements risk management in most, if not all, projects. Generic risk policies and procedures are formalized and widespread, and the benefits are understood at all levels of the organization, although they may not be consistently achieved in all cases. Planning and managing new projects is based on experience with similar projects. Risk Management capability is enhanced by establishing basic Risk Management discipline on a project-by-project basis. Projects implement risk management through processes that are defined, documented, practiced, trained, measured, enforced, and improvable. All projects have an assigned Risk Manager.

7.1.4 LEVEL IV - MANAGED

At the Managed Level, the organization has established a risk-aware (not risk-averse) culture that requires a proactive approach to the management of risks in all aspects of the organization. Risk information is continually developed and actively used to improve all organization processes and to increase the probability of success in projects and operations. A standard Risk Management process (or processes) is documented and used across the organization. Processes established at Level III are used (and changed, as appropriate) to help the organization's project and operations managers and technical staff perform more effectively. A group of personnel within the organization are assigned responsibility for Risk Management. This formal assignment provides for an informal communications channel to organization management outside of the Project communications channels or operational management structure. An organization-wide training program is implemented to ensure that the staff and managers have the knowledge and skills required to fulfill their assigned roles.

7.2 DETERMINING OSP RISK MANAGEMENT MATURITY LEVEL

The tool used in this evaluation is a direct derivative from the Electronic Industries Alliance (EIA) standard EIA 731, Systems Engineering Capability Maturity Model. This specific evaluation tool was used in the MSFC Risk Management Capability Maturity Assessment performed for the S&MA organization on August through November of 2002. We chose that tool because it is directly traceable to a benchmarked assessment process.

The model is a checklist of specific practices at each level that must be implemented to obtain that level. To discern whether the practice is implemented, OSP Program personnel are interviewed and asked directly "Do you do this specific practice?" To substantiate the answer,

objective evidence is also collected and taken into account. Objective evidence of risk management maturity includes, but is not limited to, such items as:

- Risk Management Plan
- Meeting agendas with risk as a topic
- Management review packages with risk content
- Baseline Top Risk List and regular revisions
- Risk management training materials, plans, and logs

The OSP Program is judged to be compliant or non-compliant for each specific practice. If compliance is shown for every specific practice in a maturity level, then the Program will be considered compliant at that level. Non-compliant practice areas are considered weaknesses and improvement plans will be developed to correct the weakness.

7.3 RISK MANAGEMENT PROCESSES AND SPECIFIC PRACTICES

Each section below lists the specific practices for the risk management processes measured in the RM-CMM evaluation. The specific practice is expected to be implemented at the maturity level provided.

7.3.1 RISK MANAGEMENT PLAN

- Level I - Plan risk management activities.
- Level II - Provide an approved risk management plan containing risk levels and expected management response for each level.
- Level III - Implement risk management for key processes within the program: design, test, manufacturing, etc.
- Level IV - Provide a procedure to measure the performance of the RM process
- Level IV - Provide a procedure to capture lessons learned.
- Level IV - Project/program manager specifies RM products that are consistent with program/project goals

7.3.2 IDENTIFICATION OF PERFORMANCE, COST, AND SCHEDULE RISKS

- Level I - Identify performance risks.

- Level II - Identify cost and schedule risks.

- Level III - Review all elements of the work breakdown structure as part of the risk identification process in order to help ensure that all program aspects have been considered.

- Level IV - Review all elements of the product breakdown structure and operations plans as part of the risk identification process in order to help ensure that all product performance and operational risks have been identified

7.3.3 RISK QUANTIFICATION

- Level I - Assess risks qualitatively.

- Level II - Assess each risk and determine the probability of occurrence and quantified consequence of impact for the program.

- Level III - Use a documented process for validating the probability and consequence, verify with alternative sources

- Level IV - When appropriate, analyze data from analogous projects, derive Bayesian relationships, derive probabilistic impacts that correlate to past experiences

- Level IV - Derive quantitative probabilistic impacts for risks against the program/projects defined goals, analyze correlations between risks and their impacts.

7.3.4 RISK ANALYSIS

- Level III - Review the analysis of risks for adequacy and completeness.

- Level III - For each risk, establish cause and effect relationships.

- Level III - Analyze each risk for potential coupling to all other identified risks.

- Level III - Develop alternative courses of action, alternatives, and fall-back positions with a recommended course of action for each risk.

- Level IV - Use collected metrics regarding identified risks and examine them in light of previous risk analyses, and when established thresholds are exceeded, initiate corrective action.

- Level IV - Perform quantitative, integrated risk analysis of the entire program or project, determine the total integrated impact to defined goals for ALL risks, and develop

decision-support products for management decision via computer modeling and simulation.

7.3.5 DEVELOPMENT OF A RISK MITIGATION STRATEGY

- Level II - Categorize risks into those that can be avoided, controlled, or accepted.
- Level III - Document risk reduction profiles and review them for appropriateness.
- Level III - Review risk mitigation (handling) including risk reduction profile for adequacy and completeness.
- Level IV - Compute the impact of the mitigation plan and compare to the expected value of the risk.
- Level IV - Develop integrated quantitative analyses from computer models and simulation that compare options of mitigation of ALL risks versus individual risks versus no mitigation against program or project defined goals.

7.3.6 IMPLEMENTATION OF THE RISK MITIGATION STRATEGY

- Level II - Implement the risk mitigation strategy for the program.
- Level III - Document risk analysis results and mitigation plans.
- Level IV - Collect metrics on the performance of the mitigation plans and the associated risks for the purpose of measuring the performance of the risk management process

7.3.7 MONITORING OF RISK MITIGATION ACTION

- Level III - Monitor and re-evaluate risks at appropriate milestones.
- Level III - Provide the results of risk monitoring activities to affected personnel and disciplines.
- Level III - Provide a mechanism for monitoring corrective actions taken and tracking open risk items to closure.
- Level IV - During risk monitoring, identify and analyze new risks and take corrective action.
- Level IV - Provide quantitative, integrated risk-based technical performance metrics for the key project metrics that track the impact of all risks against program or project defined goals.

7.3.8 COMMUNICATION AND COORDINATION OF RISK STATUS AND RISK MITIGATION EFFORTS ACROSS AFFECTED GROUPS

- Level I - Establish a communication path between the risk management team and the program management team, organizational management, and sponsors.
- Level II - Involve a multi-functional group for risk management that spans both technical and business specialties.
- Level II - Integrate risk management both vertically and horizontally across the program.
- Level III - Include risk management as a part of program formal reviews.